



PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information

Rapport de maintenance ANSSI-CC-2016/32-M01

MIFARE DESFire EV2 Version 1.6

Certificat de référence : ANSSI-CC-2016/32

Paris, le 26 septembre 2017

*Le directeur général de l'agence nationale
de la sécurité des systèmes d'information*

Guillaume POUPARD
[ORIGINAL SIGNE]



1. Références

[CER]	Rapport de certification ANSSI-CC-2016/32, MIFARE DESFire EV2, 26 mai 2016.
[MAI]	Procédure ANSSI-CC-MAI-P-01 Continuité de l'assurance.
[IAR]	MF3Dx2, TOE version 1.5 vs version 1.6, Impact Analysis Report, Rev. 1.1, 1 septembre 2017, <i>NXP SEMICONDUCTORS</i> .
[RM-Lab]	ETR Addendum - E20, MF3 and MF1 projects, E20-MF3-MF1_ETR_ADD_v1.0, 11 septembre 2017, <i>SERMA SAFETY & SECURITY</i> .
[SOG-IS]	Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0, 8 janvier 2010, Management Committee.
[CCRA]	Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, 2 juillet 2014.

2. Identification du produit maintenu

Le produit « MIFARE DESFire EV2, version 1.5 » a été initialement certifié sous la référence ANSSI-CC-2016/32 (référence [CER]).

Le produit objet de la présente maintenance est « MIFARE DESFire EV2, version 1.6 » développé par la société *NXP SEMICONDUCTORS*.

La version maintenue du produit est identifiable par la réponse à la commande GetVersion (voir [GUIDES]) dont les champs retournés ont les valeurs attendues suivantes :

Champs	Valeur attendue
VendorID	0x04
HWType	0x01
HWSubType	0x01 ou 0x02
HWMajorVersion	0x12
HWMinorVersion	0x00
SWType	0x01
SWSubType	0x01
SWMajorVersion	0x02
SWMinorVersion	0x01

3. Description des évolutions

Le rapport d'analyse d'impact de sécurité (référence [IAR]) mentionne que les modifications suivantes ont été opérées :

- corrections de bugs fonctionnels du logiciel embarqué, dont certains levaient des alarmes intempestives au vu de la spécification ;
- évolution des guides :
 - o identification de la nouvelle version du logiciel embarqué ;
 - o corrections éditoriales et évolutions mineures ;

– évolution du cycle de vie du produit par l'ajout du site suivant :

Nom du Site	Adresse	Fonction principale
<i>SPIL-CS, SILICONWARE PRECISION INDUSTRIES CO., LTD.</i>	Chung Shan Facility, No 153, Sec.3, Chung Shan Rd, Tantzy, Taichung, Taiwan, R.O.C.	Phase 4, Assemblage

– évolution du cycle de vie du produit par le retrait du site suivant :

Nom du Site	Adresse	Fonction principale
<i>NEDCARD</i>	Bijsterhuizen 25-29 NL-6604LM Wijchen, Netherlands	Phase 4, Assemblage

Le CESTI en charge de l'évaluation initiale a émis un rapport d'évaluation partielle (référence [RM-Lab]) pour réévaluer les composants d'assurance ALC impactés par l'évolution du cycle de vie du produit.

4. Fournitures applicables

Le tableau ci-dessous liste les fournitures, notamment les guides applicables au produit maintenu. La dernière colonne identifie l'origine de la prise en compte par l'ANSSI du document correspondant. En particulier, [R-M01] référence la présente maintenance.

[GUIDES]	MIFARE DESFire EV2 contactless multi-application IC, MF3Dx2 Product data sheet, Rev. 3.1, Ref. 226031, 25 avril 2017, <i>NXP SEMICONDUCTORS</i> .	[R-M01]
	MF3Dx2 Information on Guidance and Operation, Guidance and Operation Manual, Rev. 1.2, Ref. 274812, 1er août 2017, <i>NXP SEMICONDUCTORS</i> .	[R-M01]
[ST]	<p>Cible de sécurité de référence pour l'évaluation :</p> <ul style="list-style-type: none"> - MF3Dx2 MIFARE DESFire EV2 – Security Target, Rev 1.4, 1er août 2017, <i>NXP SEMICONDUCTORS</i>. <p>Pour les besoins de publication, la cible de sécurité suivante a été fournie :</p> <ul style="list-style-type: none"> - MF3Dx2 MIFARE DESFire EV2 – Security Target Lite, Rev 1.6, 1er août 2017, <i>NXP SEMICONDUCTORS</i>. 	[R-M01]
[CONF]	MIFARE DESFire EV2 – Configuration Item List, Rev 1.5, 9 août 2017, <i>NXP SEMICONDUCTORS</i> .	[R-M01]

5. Conclusions

Les évolutions listées ci-dessus sont considérées comme ayant un impact mineur. Le niveau de confiance dans cette nouvelle version du produit est donc identique à celui de la version certifiée.

6. Avertissement

Le niveau de résistance d'un produit certifié se dégrade au cours du temps. L'analyse de vulnérabilité de cette version du produit au regard des nouvelles attaques apparues depuis l'émission du certificat n'a pas été conduite dans le cadre de cette maintenance. Seule une réévaluation ou une surveillance de cette nouvelle version du produit permettrait de maintenir le niveau de confiance dans le temps.

7. Reconnaissance du certificat

Ce rapport de maintenance est émis en accord avec le document : « Assurance Continuity : CCRA Requirements, version 2.1, June 2012 ».

Reconnaissance européenne (SOG-IS)

Le certificat initial a été émis dans les conditions de l'accord du SOG-IS [SOG-IS].

L'accord de reconnaissance européen du SOG-IS de 2010 permet la reconnaissance, par les pays signataires de l'accord¹, des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique, pour les cartes à puces et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé et CC EAL7. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :



Reconnaissance internationale critères communs (CCRA)

Le certificat initial a été émis dans les conditions de l'accord du CCRA [CCRA].

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires², des certificats Critères Communs. La reconnaissance s'applique jusqu'aux composants d'assurance du niveau CC EAL 2 ainsi qu'à la famille ALC_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :



¹ La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : www.sogis.org.

² Les pays signataires de l'accord CCRA est disponible sur le site web de l'accord : www.commoncriteriaportal.org.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification@ssi.gouv.fr

La reproduction de ce document sans altération ni coupure est autorisée.